

**National Information Assurance Partnership**  
**Common Criteria Evaluation and Validation Scheme**



**Validation Report**  
**for the**  
**Cisco 8000 Series Routers running IOS-XR Version 7.3**

**Report Number:** CCEVS-VR-11274-2022

**Dated:** 11/10/2022

**Version:** 1.0

**National Institute of Standards and Technology**  
**Information Technology Laboratory**  
**100 Bureau Drive**  
**Gaithersburg, MD 20899**

**Department of Defense**  
**ATTN: NIAP, SUITE: 6982**  
**9800 Savage Road**  
**Fort Meade, MD 20755-6982**

# **ACKNOWLEDGEMENTS**

## **Validation Team**

Jerome Myers

Meredith Martinez

Marybeth Panock

Seada Mohammed

John Akins

*The Aerospace Corporation*

## **Common Criteria Testing Laboratory**

*Acumen Security, LLC*

# Table of Contents

<b>1</b>	<b>Executive Summary</b> .....	<b>5</b>
<b>2</b>	<b>Identification</b> .....	<b>6</b>
<b>3</b>	<b>Architectural Information</b> .....	<b>8</b>
3.1	TOE Overview .....	8
3.2	TOE Description.....	8
3.3	TOE Evaluated Configuration .....	8
3.3.1	Excluded Functionality .....	10
<b>3.4</b>	<b>Physical Scope of the TOE</b> .....	<b>10</b>
<b>3.5</b>	<b>Logical Scope of the TOE</b> .....	<b>11</b>
3.5.1	Security Audit .....	12
3.5.2	Cryptographic Support.....	12
3.5.3	Identification and Authentication.....	14
3.5.4	Security Management.....	14
3.5.5	Protection of the TSF .....	15
3.5.6	TOE Access.....	15
3.5.7	Trusted Path/Channels .....	15
<b>4</b>	<b>Assumptions, Threats &amp; Clarification of Scope</b> .....	<b>16</b>
4.1	Assumptions .....	16
4.2	Threats.....	18
4.3	Clarification of Scope .....	22
<b>5</b>	<b>Documentation</b> .....	<b>23</b>
<b>6</b>	<b>IT Product Testing</b> .....	<b>24</b>
6.1	Developer Testing .....	24
6.2	Evaluation Team Independent Testing.....	24
<b>7</b>	<b>Results of the Evaluation</b> .....	<b>25</b>
7.1	Evaluation of Security Target .....	25
7.2	Evaluation of Development Documentation.....	25
7.3	Evaluation of Guidance Documents.....	25
7.4	Evaluation of Life Cycle Support Activities .....	26
7.5	Evaluation of Test Documentation and the Test Activity .....	26
7.6	Vulnerability Assessment Activity .....	26
7.7	Summary of Evaluation Results .....	27
<b>8</b>	<b>Validator Comments &amp; Recommendations</b> .....	<b>28</b>
<b>9</b>	<b>Annexes</b> .....	<b>29</b>
<b>10</b>	<b>Security Target</b> .....	<b>30</b>
<b>11</b>	<b>Glossary</b> .....	<b>31</b>

**12 Bibliography..... 32**

# 1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco 8000 Series Routers running IOS-XR Version 7.3 Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security, LLC in September 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the defined in the U.S. Government Protection Profile for Security Requirements for collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP], and Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MACSEC EP) 1.2

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev.5 for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev.5), as interpreted by the Assurance Activities contained in the Protection Profile (PP). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

## 2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations.

Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (CEM) work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

**Table 1: Evaluation Identifiers**

Item	Identifier
<b>Evaluation Scheme</b>	United States NIAP Common Criteria Evaluation and Validation Scheme
<b>TOE</b>	Cisco 8000 Series Routers running IOS-XR Version 7.3
<b>Protection Profile</b>	collaborative Protection Profile for Network Devices, version 2.2e (NDcPP v2.2e) and Extended Package for MACsec Ethernet Encryption, version 1.2 (MACSEC EP v1.2)
<b>Security Target</b>	Cisco 8000 Series Routers running IOS-XR Version 7.3 Security Target, version 1.0, 21 October 2022
<b>Evaluation Technical Report</b>	Evaluation Technical Report for Cisco 8000 Series Routers running IOS-XR Version 7.3, version 0.2, 21 October 2022
<b>CC Version</b>	Version 3.1, Revision 5
<b>Conformance Result</b>	CC Part 2 Extended and CC Part 3 Conformant
<b>Sponsor</b>	Cisco Systems, Inc.
<b>Developer</b>	Cisco Systems, Inc.
<b>Common Criteria Testing Lab (CCTL)</b>	Acumen Security 2400 Research Blvd Suite #395 Rockville, MD 20850

<b>Item</b>	<b>Identifier</b>
<b>CCEVS Validators</b>	<i>The Aerospace Corporation</i> Jerome Myers Meredith Martinez Marybeth Panock Seada Mohammed John Akins

## 3 Architectural Information

### 3.1 TOE Overview

The Cisco 8000 Series Routers (herein after referred to as the C8000) is a purpose-built, routing platform that also supports MACsec encryption. The TOE includes the hardware models as defined in Table 4 of the ST.

### 3.2 TOE Description

This section provides an overview of the C8000 Target of Evaluation (TOE). This section also defines the TOE components included in the evaluated configuration of the TOE. The TOE is comprised of both software and hardware. The hardware is comprised of the following: 8808-SYS, 8812-SYS and 8818-SYS. The software is comprised of the Cisco IOS-XR 7.3.

The TOE consists of a number of components including:

- Chassis: The TOE chassis includes 16 RU (8 slot), 21 RU (12 slot) and 33 RU (18 slot) form factors. The chassis is the component of the TOE in which all other TOE components are housed.
- Route Processor (RP): A route processor in each chassis provide the advanced routing capabilities of the TOE. They also monitor and manage the other components in the C8000.
- Fabric Cards: 8808-FC, 8812-FC and 8818-FC
- Supporting Line Cards: 8800-LC-48H and 8800-LC-36FH

### 3.3 TOE Evaluated Configuration

The TOE consists of one or more physical devices as specified in section 3.4 below along with MACsec-supporting hardware (8800-LC-48H) and includes the Cisco IOS-XR software. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS-XR configuration determines how packets are handled to and from the TOE's network interfaces. The router configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internetworking device and forwarded to their configured destination.

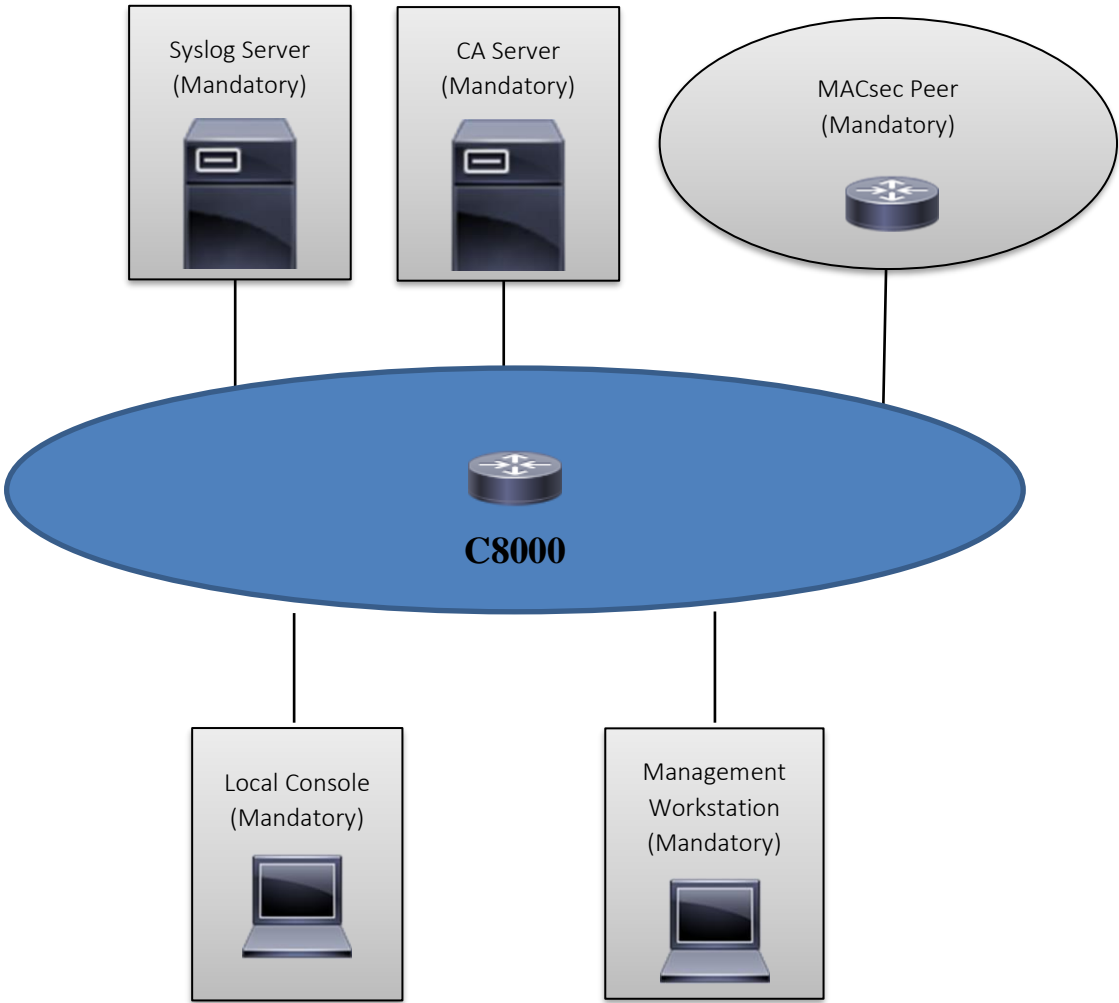
An external syslog server must be used to store audit records. The TOE authenticates those devices with X.509v3 certificates and protects communication channels with the TLS protocol. Secure remote administration is protected with SSH which is implemented with authentication failure handling.

For remote administration, a secure session using SSHv2 must be established.

The following figure provides a visual depiction of an example TOE deployment:



Figure 1 TOE Example Deployment



= TOE Boundary

Figure 1 includes the following:

- Examples of TOE Models
- The following are considered to be in the IT Environment:
  - MACsec Peer
  - Management Workstation
  - Audit (Syslog) Server
  - Local Console
  - Certificate Authority

NOTE: While Figure 1 includes several non-TOE IT environment devices, the TOE is only the C8000 device. Only one TOE device is required for deployment in an evaluated configuration.

### 3.3.1 Excluded Functionality

The following functionality is excluded from the evaluation:

**Table 2: Excluded Functionality**

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.

These services will be disabled by configuration settings. The exclusion of this functionality does not affect compliance to the NDcPP v2.2e and MACsec EP v1.2.

## 3.4 Physical Scope of the TOE




The TOE is a hardware and software solution that makes up the router models as follows:

- Chassis: 8808-SYS, 8812-SYS and 8818-SYS
- Route Processors (RP): 8800-RP
- Fabric Cards: 8808-FC, 8812-FC and 8818-FC
- Supporting Line Cards: 8800-LC-48H and 8800-LC-36FH

The network, on which they reside, is considered part of the environment. The software is pre-installed and is comprised of the Cisco IOS-XR software image Release 7.3. In addition, the software image is also downloadable from the Cisco web site. A login id and password is required to download the software image. The TOE is comprised of the following physical specifications as described in

Table 3 below:

**Table 3: Hardware Models and Specifications**

Hardware	Picture	Features
<p>Cisco 8000 Series Routers (C8000)</p> <p>8808-SYS</p> <p>8812-SYS</p> <p>8818-SYS</p> <p>8800-RP</p> <p>8808-FC</p> <p>8812-FC</p> <p>8818-FC</p> <p>8800-LC-48H</p> <p>8800-LC-36FH</p>	  <p style="text-align: center;">8800-LC-48H</p>  <p style="text-align: center;">8800-LC-36FH</p>	<p><b>Physical dimensions (H x W x D)</b></p> <ul style="list-style-type: none"> <li>8808: 28 x 17.45 x 33.73 in. (71.12 x 44.32 x 85.7 cm) – 16 RU – 8 line cards</li> <li>8812: 36.75 x 17.45 x 35.43 in. (93.345 x 44.23 x 90 cm) – 21 RU – 12 line cards</li> <li>8818: 57.75 x 17.45 x 35.43 in. (146.7 x 44.23 x 90 cm) – 33 RU – 18 line cards</li> </ul> <p><b>Route Processors (RP)</b></p> <ul style="list-style-type: none"> <li>Intel Xeon D-1530 (Broadwell) CPU</li> <li>32 GB of DRAM</li> <li>RS-232 console</li> <li>10 GbE SFP+</li> <li>1 GbE Management</li> <li>2x USB2.0</li> </ul> <p><b>Interfaces</b></p> <ul style="list-style-type: none"> <li>48 QSFP28 100 GbE</li> <li>36 QSFP56-DD 400 GbE</li> </ul> <p><b>Power</b></p> <ul style="list-style-type: none"> <li>8808 and 8812 – 9 high-voltage power supplies or 12 48V DC power supplies</li> <li>8818 - 18 high-voltage power supplies or 24 48V DC power supplies</li> </ul>

### 3.5 Logical Scope of the TOE

The TOE is comprised of several security features, as identified below.

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

These features are described in more detail in the subsections below. In addition, the TOE implements all SFRs of the NDcPP v2.2e and MACsec EP v1.2 as necessary to satisfy testing/assurance measures prescribed therein.

#### 3.5.1 Security Audit

The TOE provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The TOE generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The administrator configures auditable events, performs back-up operations and manages audit data storage. The TOE provides the administrator with a circular audit trail. The TOE is configured to transmit its audit messages to an external syslog server over an encrypted channel using TLS.

#### 3.5.2 Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality. All the algorithms claimed have CAVP certificates (Operational Environment – Intel Xeon D-1530 (Broadwell)). In addition, the TOE supports MACsec using the CoMIRA Mentor Questa Sim 10.7 processor (see Table 2 for certificate references).

**Table 4: FIPS References**

Algorithm	Description	Supported Mode	Module	CAVP Cert. #	SFR
AES	Used for symmetric encryption/decryption	CBC (128 and 256)  GCM (128 and 256)  CTR (128 and 256)  AES Key Wrap and CMAC (128 and 256)	FOM 6.2	A388	FCS_COP.1/DataEncryption FCS_COP.1(1)/KeyedHash:CMAC FCS_COP.1(2) Cryptographic Operation

Algorithm	Description	Supported Mode	Module	CAVP Cert. #	SFR
		GCM (128 and 256)	MACsec	C1668	
SHS (SHA-1, SHA-256, SHA-512)	Cryptographic hashing services	Byte Oriented	FOM 6.2	A388	FCS_COP.1/Hash
HMAC (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512)	Keyed hashing services and software integrity test	Byte Oriented	FOM 6.2	A388	FCS_COP.1/KeyedHash
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	CTR_DRBG (AES 256)	FOM 6.2	A388	FCS_RBG_EXT.1
RSA	Signature Verification and key transport	PKCS#1 v.1.5, 3072 bit key, FIPS 186-4 Key Gen	FOM 6.2	A388	FCS_CKM.1 FCS_COP.1/SigGen

The TOE provides cryptography in support of remote administrative management via SSHv2 and secures the session between the C8000 and remote syslog server using TLS.

The TOE authenticates and encrypts packets between itself and a MACsec peer. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys to protect data exchanged by the peers.

The cryptographic services provided by the TOE are described in Table 5 below:

**Table 5: TOE Provided Cryptography**

Cryptographic Method	Use within the TOE
Secure Shell Establishment	Used to establish initial SSH session.
RSA Signature Services	Used in SSH session establishment. Used in TLS session establishment. X.509 certificate signing.
SHS	Used to provide SSH traffic integrity verification Used for keyed-hash message authentication

Cryptographic Method	Use within the TOE
AES	Used to encrypt SSH session traffic. Used to encrypt TLS session traffic. Used to encrypt MACsec traffic.
RSA	Used to provide cryptographic signature services
HMAC	Used for keyed hash, integrity services in SSH session establishment.
TLS	Used to secure traffic to the syslog server.

### 3.5.3 Identification and Authentication

The TOE provides authentication services for administrative users wishing to connect to the TOEs secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as mandatory password complexity rules.

After a configurable number of incorrect login attempts, C8000 will lockout the account until a configured amount of time for lockout expires.

The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSH interfaces. The SSHv2 interface also supports authentication using SSH keys.

The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections.

### 3.5.4 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session or via a local console connection. The TOE provides the ability to securely manage all TOE administrative users, all identification and authentication, all audit functionality of the TOE, all TOE cryptographic functionality, the timestamps maintained by the TOE, and updates to the TOE. The TOE supports a privileged administrator role. Only the privileged administrator can perform the above security relevant management functions.

Administrators can create configurable login banners to be displayed at time of login and can also define an inactivity timeout for each admin interface to terminate sessions after a set period of inactivity.

### 3.5.5 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally, Cisco IOS-XR is not a general-purpose operating system and access to Cisco IOS-XR memory space is restricted to only Cisco IOS-XR functions.

The TOE is also able to detect replay of information received via secure channels (MACsec). The detection applied to network packets that terminate at the TOE, such as trusted communications between the TOE and an IT entity (e.g., MACsec peer). If replay is detected, the packets are discarded.

The TOE internally maintains the date and time. This date and time are used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually. Finally, the TOE performs testing to verify correct operation of the router itself and that of the cryptographic module.

The TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

### 3.5.6 TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE can also display a Security Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

### 3.5.7 Trusted Path/Channels

The TOE establishes a trusted path between the appliance and the CLI using SSHv2 and the syslog server using TLS. MACsec is used to secure communication channels between MACsec peers at Layer 2.

## 4 Assumptions, Threats & Clarification of Scope

### 4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

**Table 6: TOE Assumptions**

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	<p>The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.</p> <p>For vNDs, this assumption applies to the physical platform on which the VM runs.</p>
A.LIMITED_FUNCTIONALITY	<p>The device is assumed to provide networking functionality as its core function and not provide functionality/ services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality).</p> <p>In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a</p>



Assumption	Assumption Definition
	single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality.
A.NO_THRU_TRAFFIC_PROTECTION	<p>A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND ePP. It is assumed that this protection will be covered by ePPs for particular types of network devices (e.g, firewall).<sup>1</sup></p>
A.TRUSTED_ADMINISTRATOR	<p>The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.</p> <p>For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', 'trusted</p>

---

<sup>1</sup> Assumption does not apply per MACsec EP v1.2

Assumption	Assumption Definition
	CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

## 4.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

**Table 7: Threats**

Threat	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the Network Device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or

Threat	Threat Definition
	<p>performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.</p>
<p>T.WEAK_CRYPTOGRAPHY</p>	<p>Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.</p>
<p>T.WEAK_AUTHENTICATION_ENDPOINTS</p>	<p>Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and</p>

Threat	Threat Definition
	potentially the Network Device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.

Threat	Threat Definition
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
T.DATA_INTEGRITY	An attacker may modify data transmitted over the MACsec channel in a way that is not detected by the recipient.
T.NETWORK_ACCESS	An attacker may send traffic through the TOE that enables them to access devices in the TOE's Operational Environment without authorization.
T.UNTRUSTED_COMMUNICATION_CHANNELS	An attacker may acquire sensitive TOE or user data that is transmitted to or from the TOE because an untrusted communication channel causes a disclosure of data in transit.

### 4.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the NDcPP v2.2e and MACSEC EP v1.2.
- Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs, and reflected in the Security Functional Requirements (SFRs) in the ST. Any additional security related functional capabilities included in the product were not covered by this evaluation. See Section 3.3 for excluded functionalities.
- This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
- The TOE must be installed, configured, and managed as described in the documentation referenced in Section 5 of this Validation Report.

## 5 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Cisco 8000 Series Routers running IOS-XR Version 7.3 Common Criteria Operational User Guidance, version 1.1, 08 November 2022
- System Setup Guide for Cisco 8000 Series Routers, IOS XR Release 7.3.x, 28 October 2022
- Software Installation Guide for Cisco 8000 Series Routers, 26 October 2022
- Hardware Installation Guide for Cisco 8800 Series Routers, 25 October 2022
- System Security Configuration Guide for Cisco 8000 Series Routers, 04 November 2022

This is also provided for initial setup purposes. To use the product in the evaluated configuration, the product must be configured as specified in these guides.

Any additional customer documentation provided with the product, or that which may be available online was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated. Consumers are encouraged to download these listed guidance documents from the NIAP website.

## **6 IT Product Testing**

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Reports for Cisco 8000 Series Routers running IOS-XR Version 7.3, which is not publicly available. Section 4 of the Assurance Activities Report provides testbed configuration diagrams and a list of test tools and versions used during the evaluation.

### **6.1 Developer Testing**

No evidence of developer testing is required in the Assurance Activities for this product.

### **6.2 Evaluation Team Independent Testing**

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the NDcPP v2.2e and MACSEC EP 1.2. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here.



## **7 Results of the Evaluation**

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR) and summarized in the Assurance Activities Report (AAR), which is publicly available. The reader of this document can assume that all activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 Rev.5 and CEM version 3.1 Rev.5. The evaluation determined the Cisco 8000 Series Routers running IOS-XR Version 7.3 to be Part 2 extended and Part 3 conformant, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the NDcPP v2.2e and MACSEC EP v1.2.

### **7.1 Evaluation of Security Target**

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Cisco 8000 Series Routers running IOS-XR Version 7.3 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the NDcPP v2.2e and MACSEC EP v1.2.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

### **7.2 Evaluation of Development Documentation**

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the NDcPP v2.2e and MACSEC EP v1.2 related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

### **7.3 Evaluation of Guidance Documents**

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the

evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the NDcPP v2.2e and MACSECEP v1.2 related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

#### **7.4 Evaluation of Life Cycle Support Activities**

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

#### **7.5 Evaluation of Test Documentation and the Test Activity**

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the NDcPP v2.2e and MACSEC EP v1.2 and recorded the results in a Test Report, summarized in the ETR and AAR.

The validator reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDcPP v2.2e and MACSEC EP v1.2, and that the conclusion reached by the evaluation team was justified.

#### **7.6 Vulnerability Assessment Activity**

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities on 19 September 2022 and again on 23 October 2022. Fuzz testing was also performed, and neither of these activities revealed any vulnerabilities associated with the TOE.

Section 16.1.6 titled ‘AVA\_VAN.1 Vulnerability Survey’ of the Assurance Activities Report provides an overview of the vulnerability assessment performed for the TOE.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the NDcPP v2.2e and MACSEC EP v1.2, and that the conclusion reached by the evaluation team was justified.

## **7.7 Summary of Evaluation Results**

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the NDcPP v2.2e and MACSEC EP v1.2, and correctly verified that the product meets the claims in the ST.

## **8 Validator Comments & Recommendations**

All validator comments are addressed in Section 4, Assumptions, Threats & Clarification of Scope.

## **9 Annexes**

Not applicable.

## **10 Security Target**

Cisco 8000 Series Routers running IOS-XR Version 7.3 Security Target, version 1.0, 21 October 2022.

## 11 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

## 12 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. Collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP]
6. Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MACSECEP) 1.2
7. Cisco 8000 Series Routers running IOS-XR Version 7.3 Security Target, version 1.0, 21 October 2022
8. Cisco 8000 Series Routers running IOS-XR Version 7.3 Common Criteria Operational User Guidance, version 1.1, 08 November 2022
9. Assurance Activity Report for Cisco 8000 Series Routers running IOS-XR Version 7.3, version 0.3, 07 November 2022
10. Evaluation Technical Report for Cisco 8000 Series Routers running IOS-XR Version 7.3, version 0.2, 21 October 2022